CLAIMS:

1. A system for the authentication by a card-issuing financial institution of identifying information of a card-holding user of a public data network, including:

a secure data entry device connected to the public data network; and

a gateway device connected to the public data network and to a private data network used for transmitting messages between financial institutions;

wherein the secure data entry device includes means for the user to enter identifying information of a card issued by the financial institution, and means for transmitting the identifying information in a secure manner over the public data network to the gateway device; and

wherein the gateway device includes means for transmitting the identifying information to the card-issuing financial institution and for receiving an approval response from the card-issuing financial institution over the private data network;

whereby the approval response provides authentication of the identifying information by the card-issuing financial institution.

2. The system of claim 1 wherein the public data network is the Internet.

3. The system of claim 1 or 2 wherein the secure data entry device is connected to the public data network via a personal computer.

4. The system of any one of the preceding claims wherein the private data network is an inter-bank network used for the transferral of electronic transaction data.

5. The system of claim 4 wherein the private data network is provided via a dedicated network operated for the sole purpose of conducting electronic financial transactions.

6. The system of claim 4 wherein the private data network is a virtual private network operated for the purpose of conducting electronic financial transactions via a host public data network.

7. The system of any one of the preceding claims wherein the secure data entry device further includes: a card reader for reading relevant information stored on the user's card; and a keypad to enable the user to enter data into the system.

8. The system of claim 7 wherein the card reader is able to read one or both of ISO 7816 'smart card' or ISO 7811 'mag stripe' type cards.

9. The system of claim 7 wherein data entered by the user includes a Personal Identification Number associated with the card.

10. The system of any one of the preceding claims wherein said identifying information includes one or more of:

the Primary Account Number associated with the card;
the expiry date of the card; and
the user's Personal Identification Number associated with the card.

11. The system of any one of the preceding claims wherein the identifying information is transmitted using a standard transaction message format compliant to ISO 8583.

12. The system of claim 11 wherein the ISO 8583 message used is one of an '0200' financial presentment message, and or an '0104' authorisation message.

13. The system of any one of the preceding claims wherein the gateway device also includes means for transmitting the approval response to the secure data entry device.

14. The system of claim 13 wherein the secure data entry device further includes means for deriving from the approval response verifiable proof that the customer's identifying information has been authenticated by the card-issuing financial institution.

15. The system of claim 14 wherein said proof is an authentication data block, consisting of data computed in a secure manner from the approval sent from the card-issuing bank.

16. The system of claim 15 wherein the data block is a whole or truncated encryption of the approval message derived using an encryption key stored securely within the secure data entry device.

17. The system of any one of the preceding claims wherein the gateway device further includes means to generate a replacement card number upon receipt of the approval response from the card-issuing institution.

18. The system of claim 17 wherein the replacement card number is transmitted to the secure data entry device over the public data network.

19. The system of claim 17 or 18 wherein the replacement card number is generated dynamically for use in a single transaction.

20. The system of claim 17 or 18 wherein the replacement card number is maintained and used for multiple transactions.

21. The system of any one of claims 17 to 20 wherein supplementary details of a transaction are also be transmitted to the gateway device by the secure data entry device, and wherein said supplementary details include one or more of the transaction amount and a merchant identification.

22. The system of claim 21 wherein said supplementary details are transmitted to the gateway device in the transaction message carrying the identifying information.

23. The system of any one of claims 17 to 22 wherein the Bank Identification Number of the replacement card number may be selected such that the payment transaction is routed through the gateway device on the private data network before being sent to the card-issuing financial institution.

24. The system of any one of claims 17 to 22 wherein the Bank Identification Number of the replacement card number may be selected such that the payment transaction is directed over the private data network to the gateway device by identifying the gateway device as a card-issuing institution of the replacement card number.

25. The system of any one of claims 17 to 24 wherein the gateway device further includes:

means for receiving payment transaction messages from the private data network;

means for modifying received payment transaction messages; and

means for transmitting said modified payment transaction messages to the card-issuing financial institution;

whereby the gateway device is able to substitute actual card numbers for replacement card numbers before transmitting received payment transaction messages to the card-issuing financial institution.

26. The system of any one of claims 17 to 25 wherein the gateway device further includes a database of replacement card numbers including corresponding actual card numbers and supplementary transaction details.

27. A method for the authentication by a card-issuing financial institution of identifying information of a card-holding user of a public data network, including the steps of:

providing a secure data entry device connected to the public data network;

providing a gateway device connected to the public data network and to a private data network used for transmitting messages between financial institutions;

the user entering identifying information of a card issued by the card issuing financial institution into the secure data entry device;

transmitting the identifying information in a secure manner over the public data network to the gateway device;

transmitting the identifying information to the card-issuing financial institution; and

receiving an approval response from the card-issuing financial institution over the private data network;

whereby the approval response provides authentication of the identifying information by the card-issuing financial institution.

28. A process for the authentication, by a card-issuing financial institution, of identifying information of a card-holding user of a public data network, the process including the following steps:

providing a secure data entry device connected to the public data network; and

providing a gateway device connected to the public data network and to a private data network used for transmitting messages between financial institutions;

transmitting the identifying information in a secure manner over the public data network to the gateway device;

transmitting the identifying information to the card-issuing financial institution; and

receiving an approval response from the card-issuing financial institution over the private data network;

whereby the approval response provides authentication of the identifying information by the card-issuing financial institution.